Università Politecnica delle Marche

Facoltà di Ingegneria

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione

Social Network Analysis

Principali incidenti informatici avvenuti tra il 2005 e il 2020

Docenti
Prof. Ursino Domenico
Dott. Buratti Christopher

Componenti del gruppo
Dott. Tempera Fabio
Dott. Marcianesi Luca
Dott. Vianello Gabriele

ANNO ACCADEMICO 2024-2025

Indice

Elenco delle figure

Elenco delle tabelle

1 Introduzione

1.1 Social Newtork Analysis (SNA)

La **Social Network Analysis (SNA)** è un approccio interdisciplinare che studia le strutture delle relazioni tra entità, chiamate **nodi**, e le connessioni tra di esse, chiamate **archi**. Viene utilizzata per analizzare e visualizzare reti sociali, dove i nodi possono rappresentare persone, organizzazioni o concetti, e gli archi possono rappresentare relazioni come amicizie, collaborazioni, scambi di informazioni o influenze.

La Social Network Analysis (SNA), diversamente da quanto si crede, nasce prima dell'avvento dei più famosi social network come Twitter e Facebook. Grazie alla sua natura basata sull'analisi dei grafi è stata utilizzata molto nei social media ed è diventata estremamente famosa con il passare degli anni. La sociologia sta alla base di questa tecnica di Data Science.

Obiettivi della SNA

Gli obiettivi principali della SNA includono:

- **Comprendere le dinamiche relazionali**: individuare modelli di interazione per capire come si organizzano e si sviluppano le relazioni sociali.
- **Identificare attori chiave**: scoprire nodi centrali o influenti, come leader informali o ponti tra diversi gruppi.
- **Valutare la coesione**: misurare quanto una rete sia coesa (densa) o frammentata per comprendere la resilienza del sistema sociale.
- **Prevedere la diffusione di idee o influenze**: studiare fenomeni come la viralità di un contenuto o la propagazione di malattie.

Elementi Fondamentali della SNA

1. **Nodi (o Vertici)**: Rappresentano le entità in una rete (persone, gruppi, organizzazioni, ecc.).

2. **Archi (o Collegamenti)**: Rappresentano le relazioni o interazioni tra i nodi.
3. **Grafi**: La rappresentazione visuale della rete come un insieme di nodi e archi.

Applicazioni della SNA

La SNA è applicata in diversi campi, tra cui:

- **Sociologia**: analisi di gruppi sociali, reti di amicizia, influenze sociali.
- **Business**: identificazione di leader informali, analisi della struttura organizzativa, studio delle catene di valore.
- **Marketing**: studio della diffusione di campagne pubblicitarie, influencer marketing.
- **Epidemiologia**: analisi della diffusione di malattie infettive.
- **Informatica**: studio delle reti di comunicazione, come Internet o i social media.
- **Criminologia**: indagine su reti di criminalità organizzata.

1.2 NetworkX

In questo progetto si farà uso della libreria *NetworkX* per lo studio delle reti secondo la teoria dei grafi. NetworkX fornisce diversi strumenti, grafici e non, per lo studio della struttura delle reti sociali e permette di lavorare con grandi dataset, in modo rapido ed efficiente.

Figura 1.1: Logo NetworkX

2 Dataset

2.1 Presentazione del dataset

Il dataset scelto per lo svolgimento della Social Network Analysis (SNA) contiene una raccolta dei principali incidenti informatici avvenuti tra il 2005 e il 2020. È possibile scaricare il dataset da Kaggle al seguente link: Cyber incidents 2005 to 2020.

All'interno del file sono presenti diversi attributi, ma per la costruzione del grafo i più significativi sono:

- *Victims*: una stringa che descrive la vittima dell'attacco (es. "Austrian Foreign Ministry", "Chinese Ministry of Emergency Management")
- *Sponsor*: una stringa che identifica la nazione che si sospetta abbia finanziato o sponsorizzato l'attacco (es. "Iran (Islamic Republic of)", "United States")
- *Title*: descrizione dell'incidente
- *Type*: categoria dell'attacco (es. espionaggio, sabotaggi, etc.)
- *Category*: categoria dell'incidente

Poiché il dataset non è concepito nativamente per Social Network Analysis, è necessario ricondurre i dati alla struttura di un grafo orientato pesato in cui:

- **Nodi**: Rappresentano le nazioni (identificate da codici ISO 2 lettere)
- **Archi orientati**: Rappresentano relazioni di attacco, dove un arco da nazione A a nazione B indica che A ha attaccato B
- **Pesi**: Rappresentano il numero di incidenti registrati tra due nazioni

Nello specifico:

- *Arco entrante*: Un arco entrante nel nodo corrisponde a subire un attacco informatico

- *Arco uscente*: Un arco uscente corrisponde a lanciare un attacco verso un'altra nazione

2.2 Operazioni di preprocessing svolte sul dataset

Per rendere il dataset adatto alla SNA è fondamentale adattare i dati alla struttura di un grafo. Per far ciò è stato fondamentale elaborare le colonne *Victims* e *Sponsor* in modo da rendere i valori di questi attributi standard, normalizzati e facilmente interpretabili per l'analisi.

Il preprocessing è articolato in due fasi principali:

- *Pulizia*: I record in cui l'attributo Victims non è valorizzato sono stati eliminati per garantire che tutti gli archi del grafo siano ben definiti.
- *Normalizzazione*: I valori degli attributi Victims e Sponsor non sono sempre nomi di nazioni ma possono essere entità specifiche (es. "Austrian Foreign Ministry", "Wuhan government") o variazioni di nomi nazionali (es. "Palestine, State of", "Islamic Republic of Iran"). Questi necessitano di un tipo di elaborazione specializzato.

2.3 Sistema di Normalizzazione Ibrido (Regex + AI)

La normalizzazione dei nomi di paesi utilizza un approccio a due livelli, combinando tecniche deterministiche e intelligenza artificiale:

2.3.1 Fase 1: Normalizzazione Euristica (Regex)

Un algoritmo basato su pattern matching e regole euristiche effettua il mapping di oltre 150 variazioni di nomi di paesi verso i nomi canonici ISO. Questo include:

- Variazioni comuni di nomi (es. "USA" $\rightarrow$ "United States", "PRC" $\rightarrow$ "China")
- Nomi di città che fungono da proxy per il paese (es. "Wuhan", "Beijing" $\rightarrow$ "China")
- Gestione di ambiguità geopolitiche (es. distinzione tra "Korea (Democratic People's Republic)" e "Korea (Republic of)" in base ai keyword presenti nel testo)
- Mapping di entità geografiche non-standard (es. "West Bank", "Gaza" $\rightarrow$ "Palestine")

Tabella 2.1: Esempi di normalizzazione Victims e Sponsor

Testo Originale	**Paese Normalizzato**
Austrian Foreign Ministry	Austria
Wuhan government, Chinese Ministry of Emergency Management	China
Israeli Defense Forces (IDF) soldiers	Israel
Employees of the U.S. government	United States
Iran (Islamic Republic of)	Iran
Palestine, State of	Palestine
Korean People's Army (Democratic People's Republic of Korea)	North Korea

2.3.2 Fase 2: Arricchimento tramite LLM (Fallback)

Per i record che non possono essere normalizzati euristicamente (classificati come "Unknown"), il sistema invoca un modello linguistico locale (Qwen via LM Studio) tramite il modulo `utils.llm_client`. L'LLM estrae il paese dal testo descrittivo non strutturato, permettendo una normalizzazione più accurata e contestuale. Questo approccio ibrido garantisce un'alta copertura di dati pur mantenendo affidabilità deterministica.

2.4 Descrizione e analisi esplorativa del grafo

Dopo il preprocessing e la normalizzazione, il dataset è stato trasformato in un grafo orientato pesato. Di seguito sono riportate le caratteristiche strutturali del grafo:

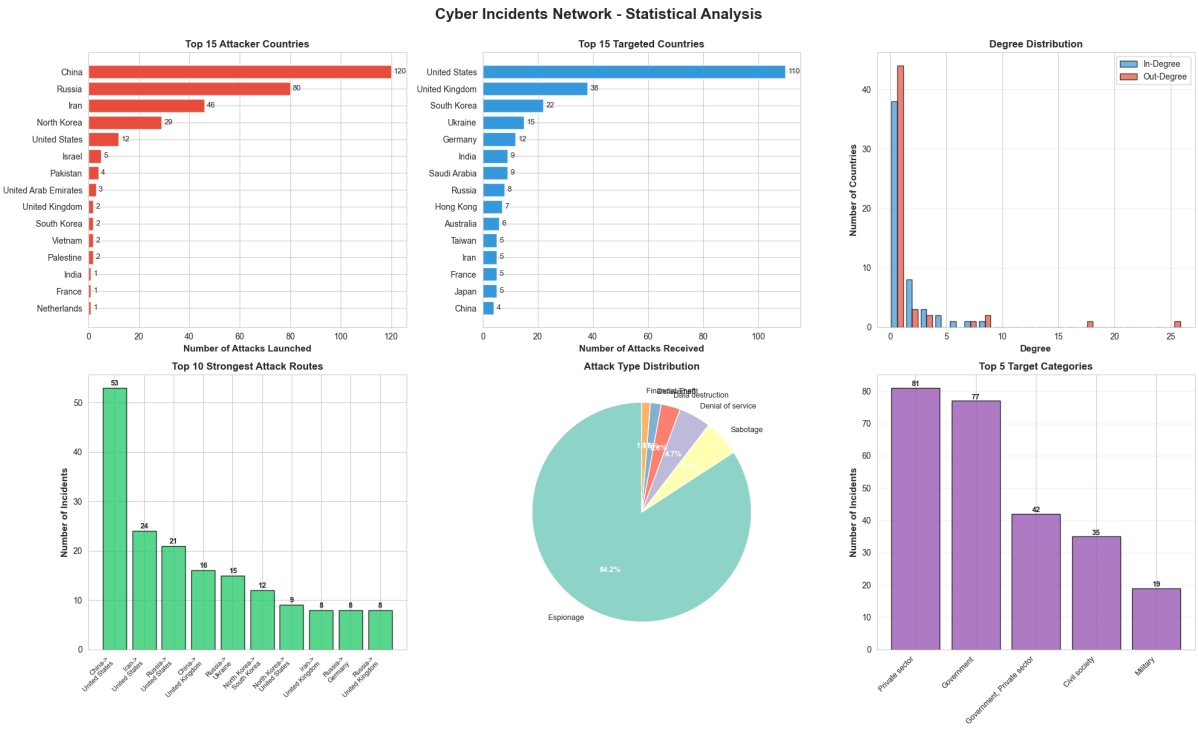

Figura 2.1: Statistiche principali del grafo degli incidenti cyber

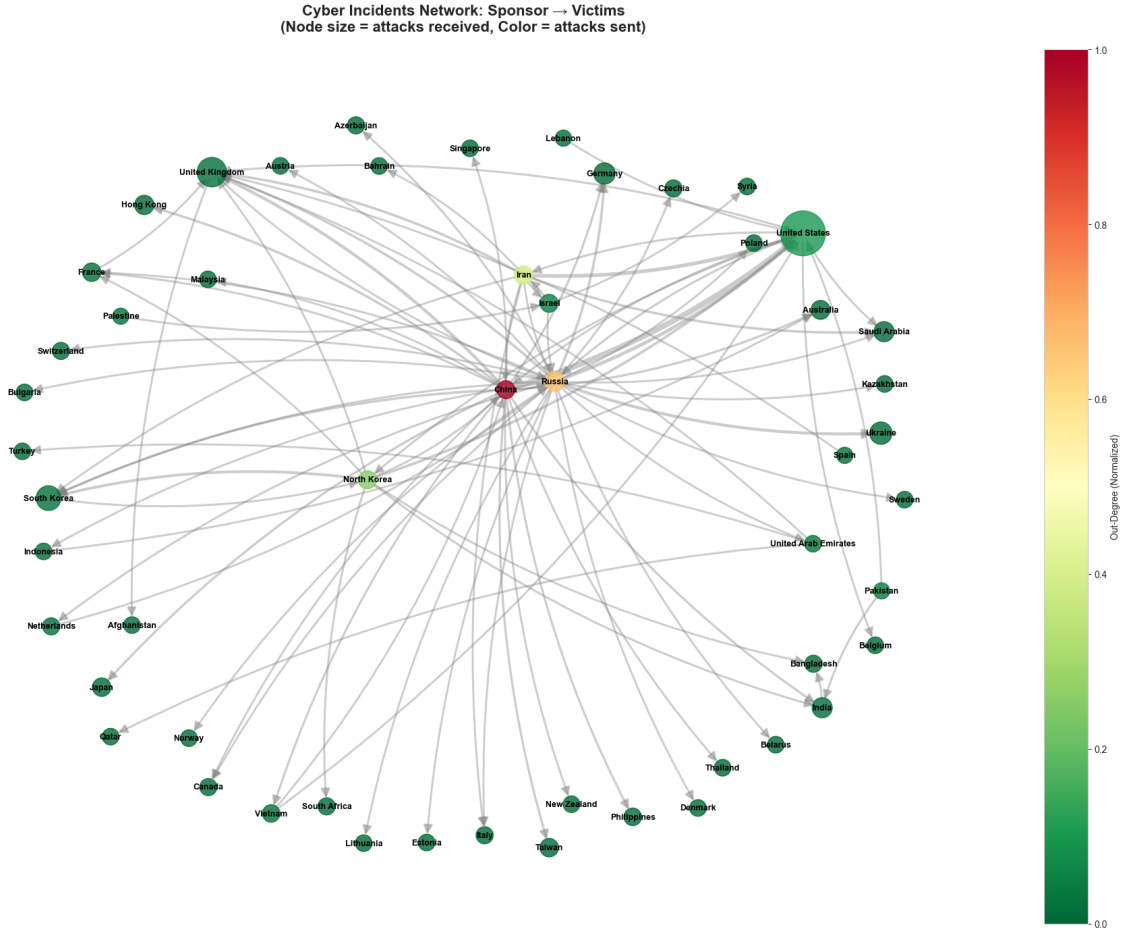

Figura 2.2: Rappresentazione del grafo attraverso Spring Layout

Il grafo risultante contiene nodi rappresentanti i paesi coinvolti negli attacchi e archi pesati che rappresentano le relazioni di attacco. L'analisi di queste proprietà topologiche fornisce insight fondamentali sulla struttura della rete di incidenti cyber globali.

3 Analisi delle Misure di Centralità

All'interno di una rete di incidenti cyber, una delle prime analisi da compiere è quella di quantificare il potere, l'influenza e la vulnerabilità dei singoli nodi (paesi). Queste caratteristiche, fondamentali per comprendere la struttura e il funzionamento della rete geopolitica cybernetica, sono determinate dalle connessioni tra i nodi stessi.

3.1 Degree Centrality

La *Degree Centrality* misura il numero di connessioni dirette che un nodo possiede all'interno di una rete. Un nodo con un alto grado è un nodo molto attivo, che interagisce direttamente con molte altre entità della rete.

3.1.1 In-Degree Centrality

La *In-Degree Centrality* misura il numero di attacchi entranti verso un paese. Un paese con alta In-Degree Centrality è una vittima frequente di incidenti cyber e rappresenta un bersaglio privilegiato nell'ecosistema dei conflitti cyber globali.

Nel contesto degli incidenti cyber:

- Valori alti indicano paesi altamente vulnerabili o bersagli strategici
- Correla con infrastrutture critiche e importanza geopolitica
- Identifica le vittime principali nei conflitti cyber internazionali

Tabella 3.1: Risultati

United Kingdom	0.150943
United States	0.132075
Russia	0.113208
South Korea	0.075472
China	0.075472
France	0.056604
India	0.056604
Saudi Arabia	0.056604
Canada	0.037736
Germany	0.037736

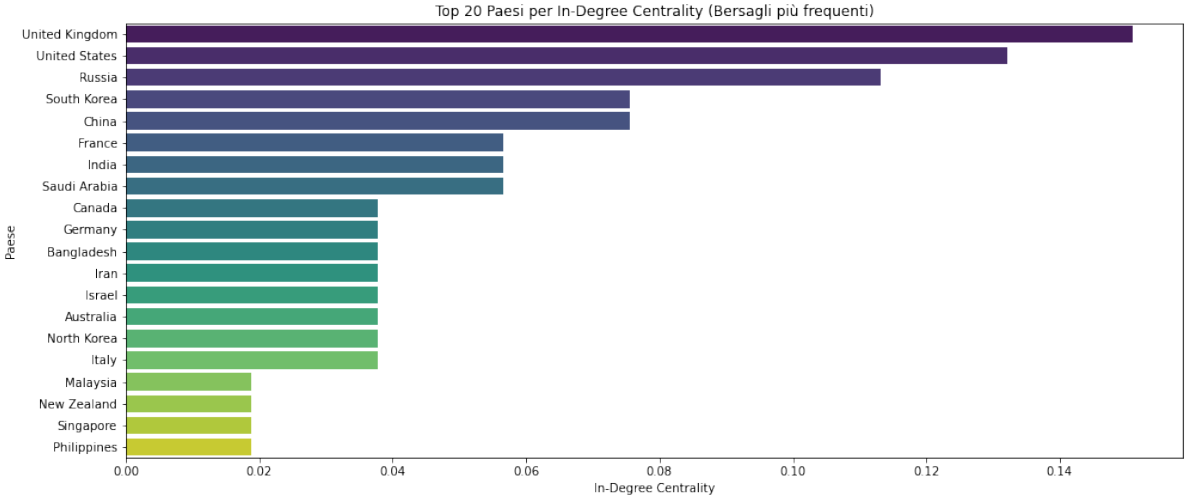

Figura 3.1: Visualizzazione dei top 20 paesi per in-degree centrality

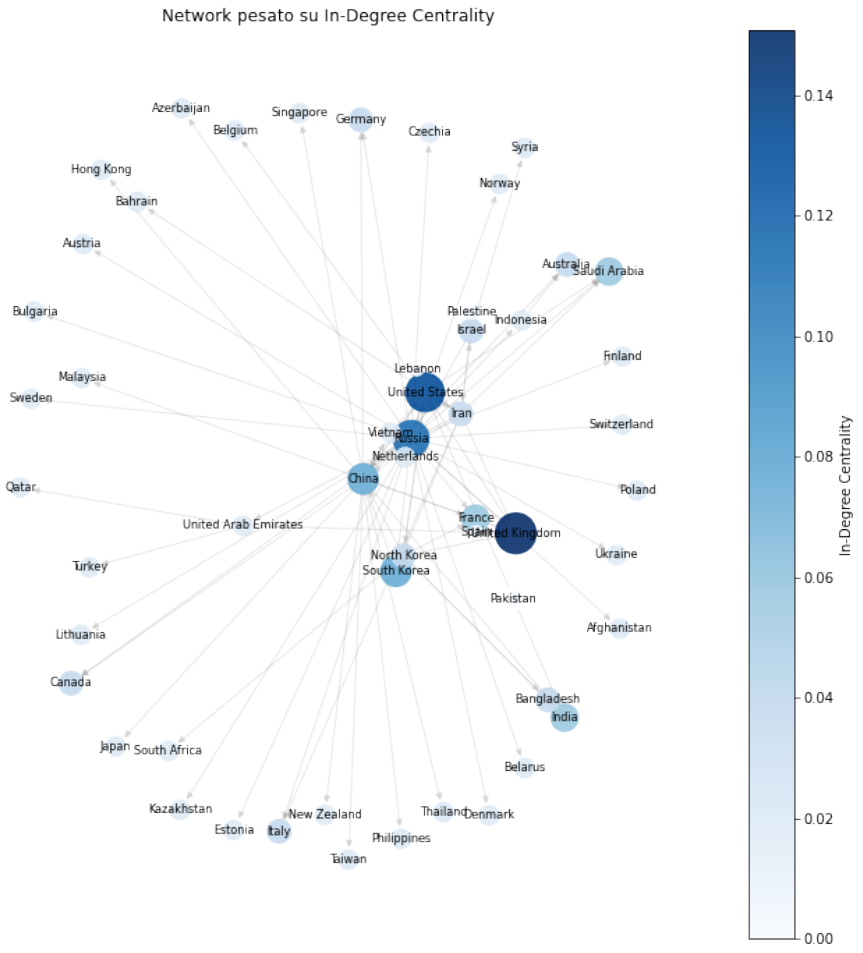

Figura 3.2: Visualizzazione grafo pesato sull’in-degree centrality

3.1.2 Out-Degree Centrality

La *Out-Degree Centrality* misura il numero di attacchi generati da un paese verso altri paesi. Un paese con alta Out-Degree Centrality è un attaccante attivo e rappresenta una fonte primaria di minacce nel panorama cyber internazionale.

Nel contesto degli incidenti cyber:

- Valori alti indicano paesi che conducono operazioni cyber aggressive
- Correlati con capacità cyber offensive e intenzioni geopolitiche
- Identificano gli attori principali negli scenari di guerra cyber

Tabella 3.2: Risultati

Russia	0.490566
China	0.339623
Iran	0.169811
North Korea	0.150943
United States	0.132075
Israel	0.056604
United Arab Emirates	0.056604
Pakistan	0.037736
Vietnam	0.037736
United Kingdom	0.037736

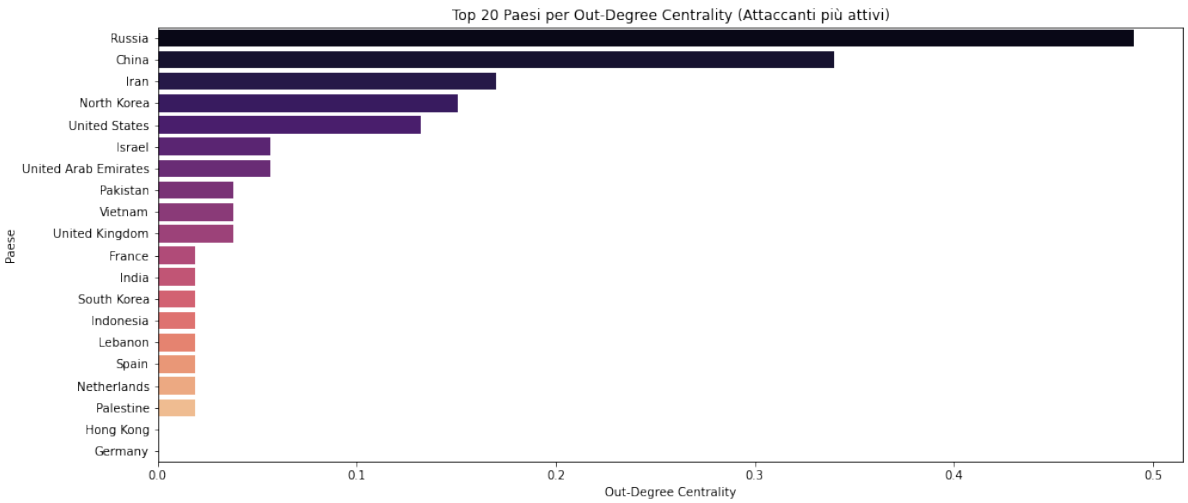

Figura 3.3: Visualizzazione dei top 20 paesi per out-degree centrality

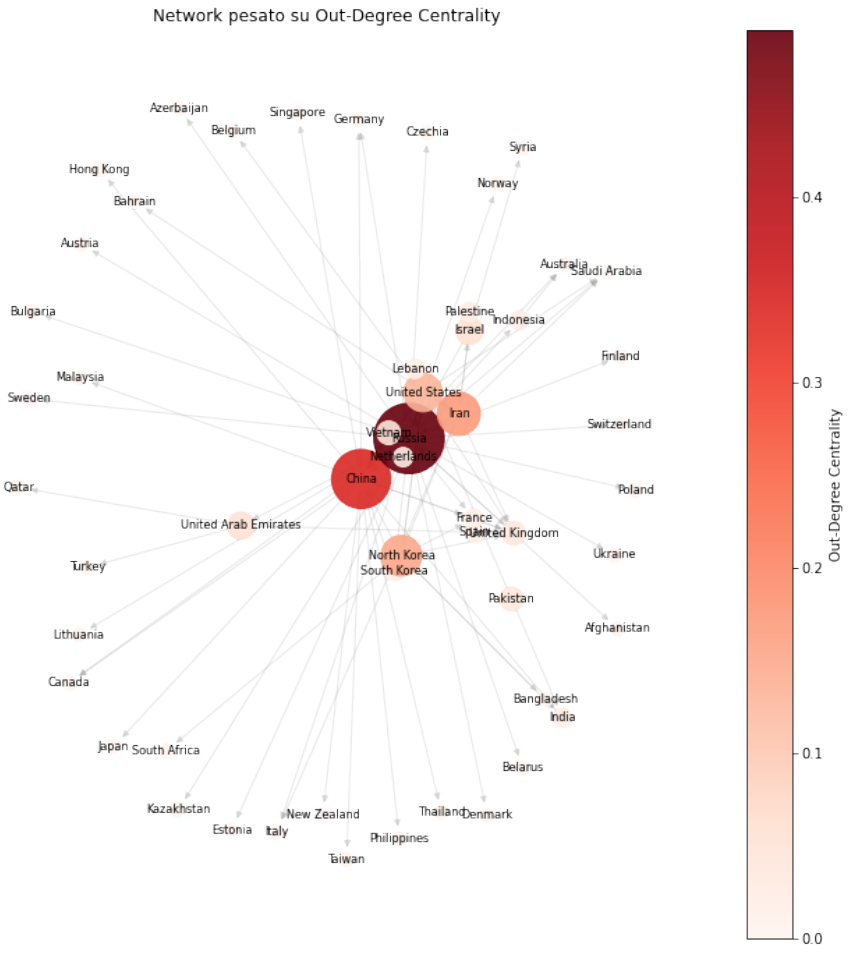

Figura 3.4: Visualizzazione grafo pesato sull'out-degree centrality

3.2 Betweenness Centrality

La *Betweenness Centrality* è una metrica che consente di valutare il potere o l'influenza di un nodo nella rete, basandosi su un principio differente rispetto alle misure precedenti. Un nodo con un'alta *Betweenness Centrality* funge da "ponte" o "intermediario" nelle rotte di attacco.

Questa metrica è particolarmente significativa nel contesto cyber perché:

- Identifica paesi che fungono da hub nelle catene di attacco
- Rivela infrastrutture critiche per la propagazione di minacce
- Espone punti di vulnerabilità strategica nella rete globale
- Paesi con alta betweenness sono "colli di bottiglia" nella topologia della rete cyber

Tabella 3.3: Risultati

Russia	0.166987
United States	0.094448
China	0.069237
United Kingdom	0.061502
North Korea	0.028852
Iran	0.028042
Israel	0.022859
United Arab Emirates	0.010885
South Korea	0.005854
Indonesia	0.002540

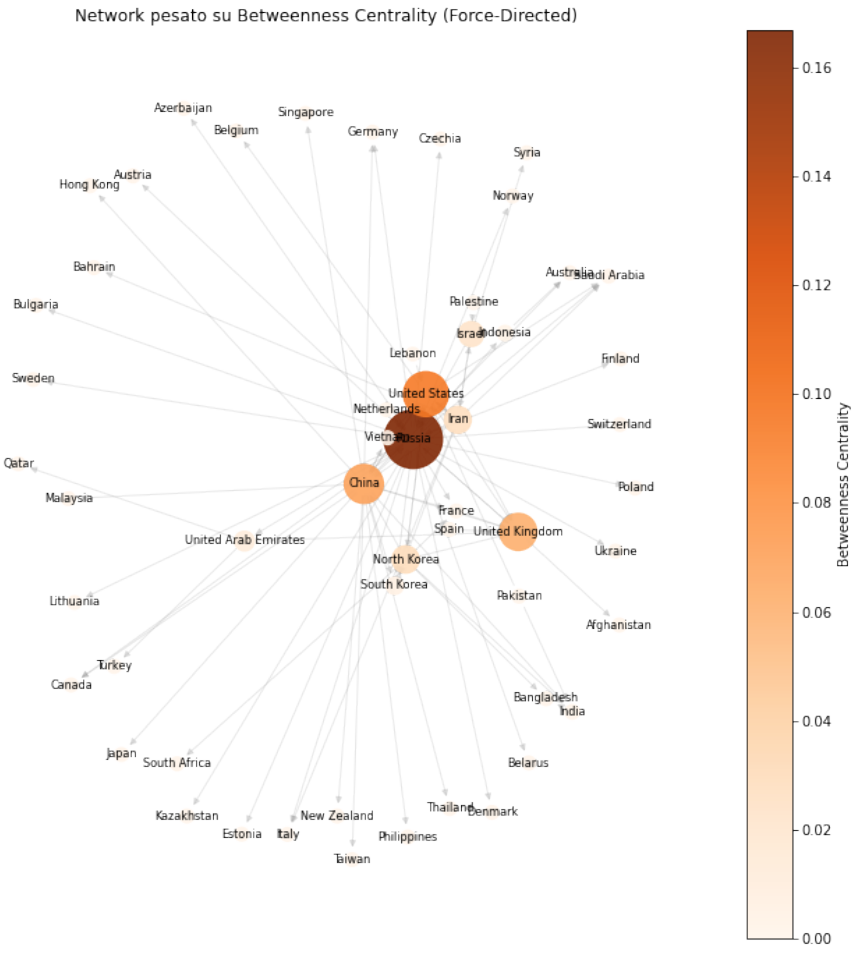

Figura 3.5: Visualizzazione grafo pesato sulla betweenness centrality

3.3 Closeness Centrality

La *Closeness Centrality* misura la capacità di un nodo di ricevere e diffondere informazioni all'interno della rete, ovvero la sua abilità nel trasferire minacce rapidamente da un nodo all'altro.

Nel contesto della cybersecurity:

- Identifica paesi centrali nella diffusione di campagne cyber
- Misura la prossimità relativa ai principali attaccanti/vittime
- Paesi con alta closeness sono nodi strategicamente posizionati nella rete

3.3.1 In-Closeness Centrality

Dato che il grafo è orientato la *In-Closeness* descrive quanto velocemente una nazione può essere raggiunta dagli altri.

Tabella 3.4: Risultati

China	0.520711
Russia	0.514794
Iran	0.487117
United States	0.481935
Israel	0.393929
North Korea	0.387196
Vietnam	0.359539
United Kingdom	0.338074
Pakistan	0.334538
Netherlands	0.333102

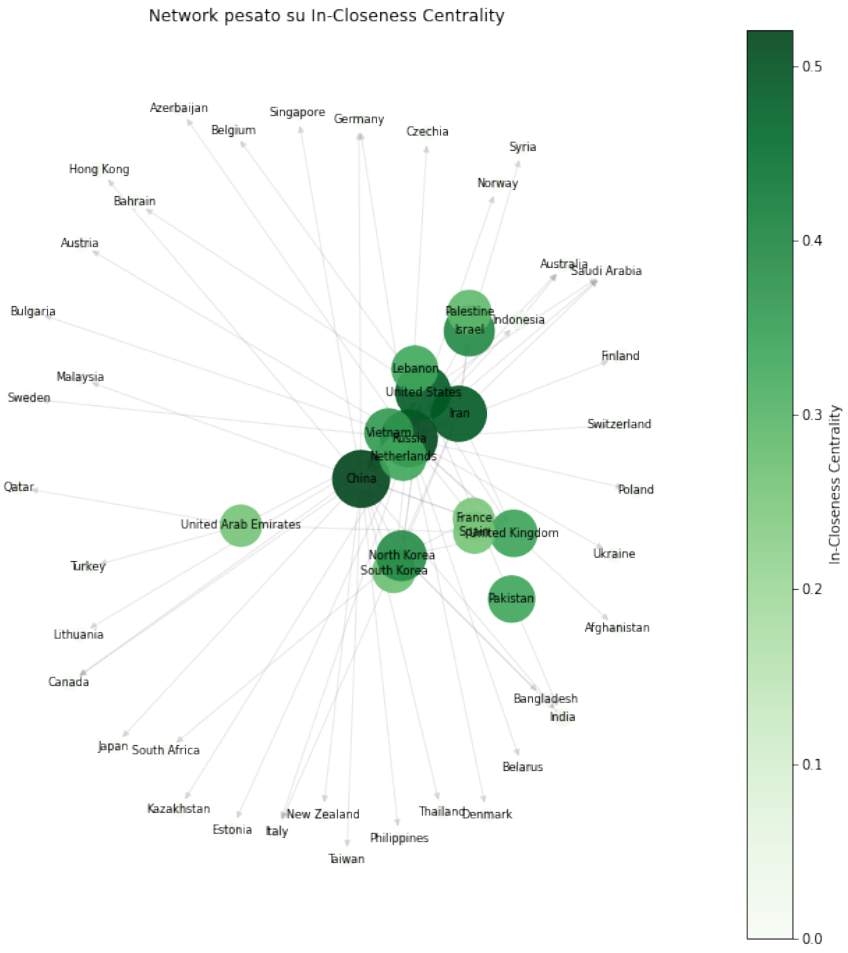

Figura 3.6: Visualizzazione grafo pesato sulla in-closeness centrality

3.3.2 Out-Closeness Centrality

Dato che il grafo è orientato la *Out-Closeness* descrive quanto una un attacco può scatenare risposte e raggiungere velocemente gli altri.

Tabella 3.5: Risultati

United Kingdom	0.184578
Russia	0.169811
United States	0.157233
Saudi Arabia	0.142064
France	0.132665
South Korea	0.132665
Germany	0.130546
Canada	0.130546
Afghanistan	0.123851
China	0.121294

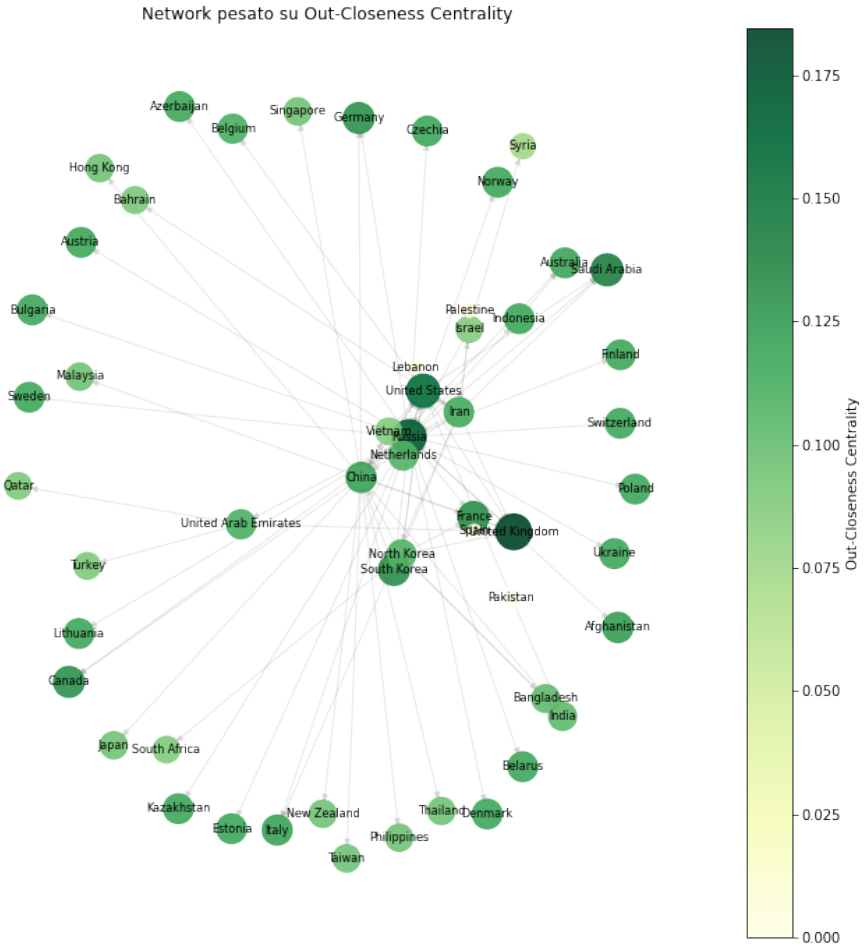

Figura 3.7: Visualizzazione grafo pesato sulla out-closeness centrality

3.4 Eigenvector Centrality

La *Eigenvector Centrality* è una metrica concepita per identificare quei nodi che, pur non essendo direttamente evidenti come altamente connessi, esercitano un'influenza significativa grazie alla qualità delle loro connessioni.

Nel contesto cyber, l'eigenvector centrality rivela:

- Paesi che, sebbene non ubiquitari in attacchi, si connettono ad altri paesi influenti
- Attori secondari ma strategicamente rilevanti nella rete
- Nodi che guadagnano influenza per associazione con paesi potenti
- Identificatori di alleanze tacite o partnership cyber

3.4.1 In-Eigenvector Centrality

Dato che il grafo è orientato un alto valore di *In-Eigenvector* indica che la nazione è bersaglio di attori cibernetici di alto livello e ben connessi.

Tabella 3.6: Risultati

United States	0.484050
Iran	0.483744
China	0.383899
North Korea	0.339582
Vietnam	0.273180
Russia	0.251518
Israel	0.231422
Pakistan	0.152351
Lebanon	0.152351
South Korea	0.106880

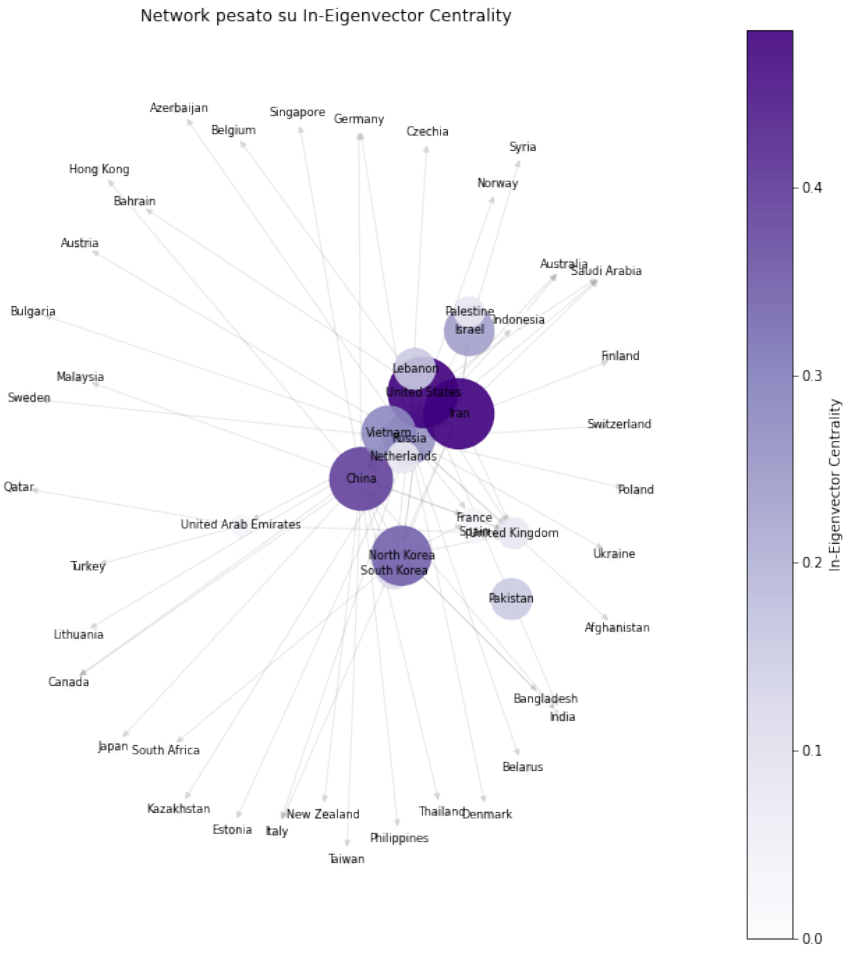

Figura 3.8: Visualizzazione grafo pesato sulla in-eigenvector centrality

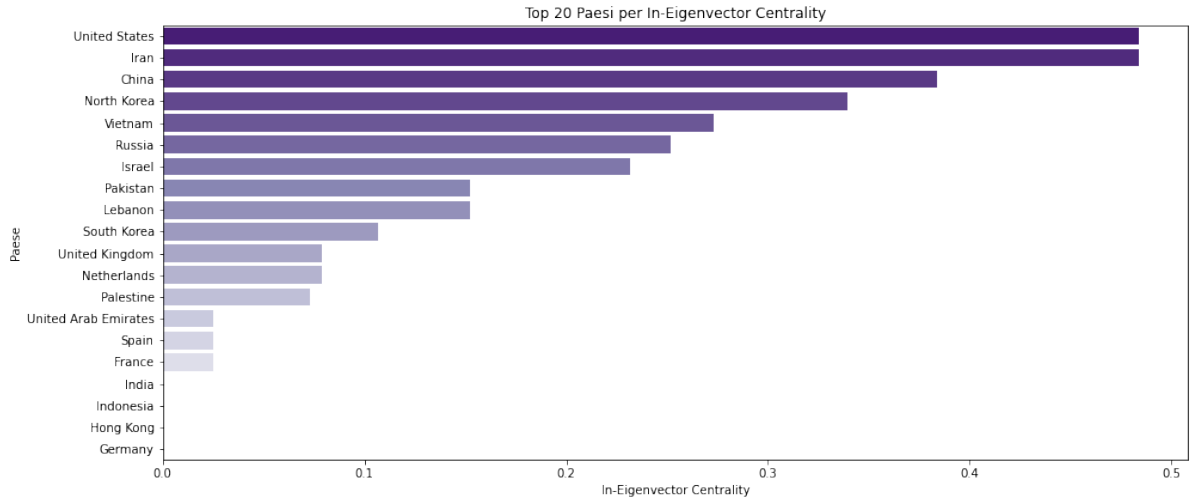

Figura 3.9: Visualizzazione dei top 20 paesi per in-eigenvector centrality

3.4.2 Out-Eigenvector Centrality

Dato che il grafo è orientato un alto valore *Out-Eigenvector* suggerisce che gli attacchi della nazione sono diretti verso obiettivi chiave e influenti della rete.

Tabella 3.7: Risultati

United Kingdom	0.436167
Russia	0.351919
United States	0.266504
South Korea	0.248449
Saudi Arabia	0.223951
France	0.219144
China	0.182256
Canada	0.168130
Germany	0.168130
North Korea	0.162080

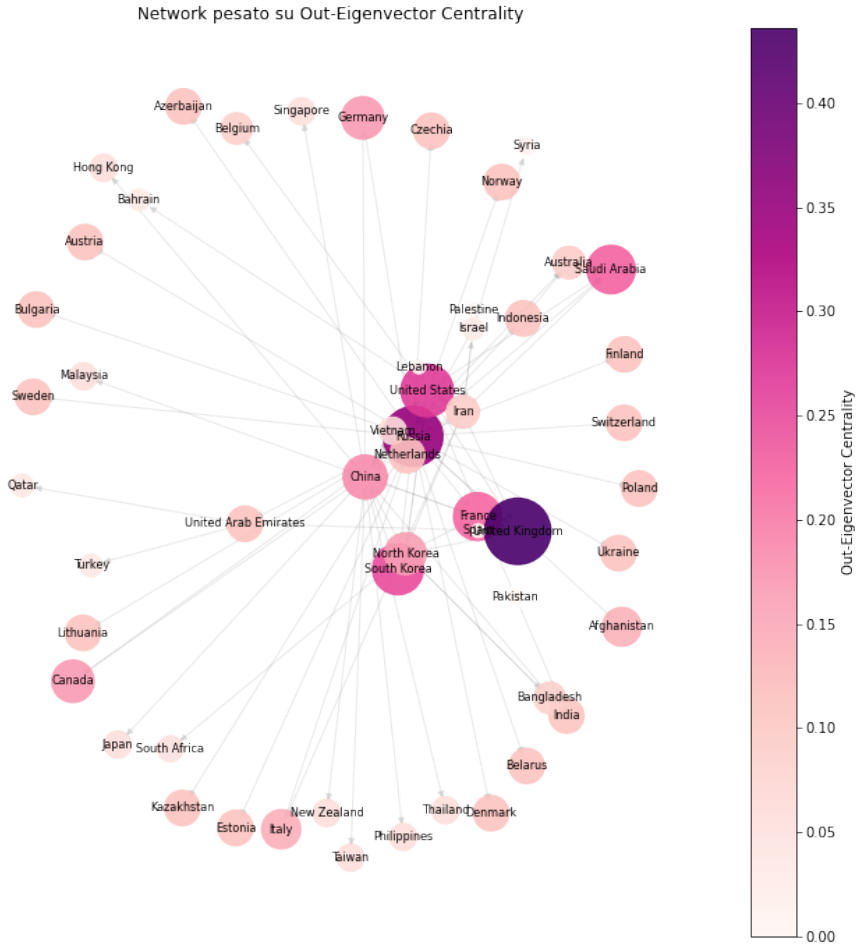

Figura 3.10: Visualizzazione grafo pesato sulla out-eigenvector centrality

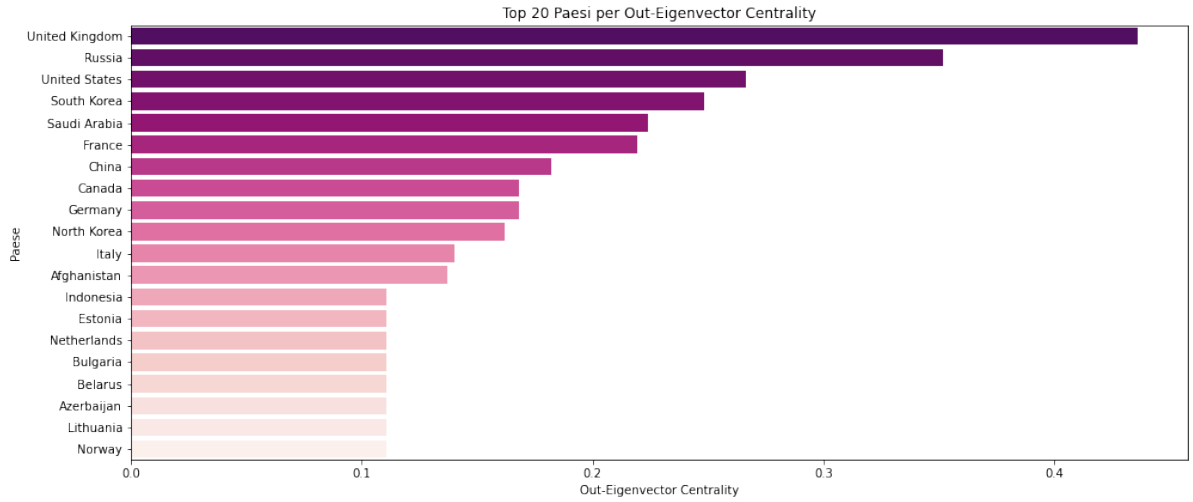

Figura 3.11: Visualizzazione dei top 20 paesi per out-eigenvector centrality

L’analisi combinata di queste metriche fornisce una visione multidimensionale della posizione di ogni paese nella rete di incidenti cyber globale, permettendo di identificare attori critici, vulnerabilità strutturali e pattern di minaccia complessi.

4 Visualizzazione e Analisi delle Strutture di Rete

In questo capitolo sono analizzati i sottografi e le strutture significative della rete di incidenti cyber globale, con focus su triadi, clique, k-core, ego network, e community detection con diversi algoritmi.

4.1 Analisi delle Triadi

Le *triadi* sono configurazioni fondamentali nella teoria dei grafi sociali. Rappresentano insiemi di tre nodi e le loro interconnessioni. Nell'analisi ci concentreremo su tre tipi di triadi applicabili al nostro contesto:

- Triadi transitive: può indicare una nazione come trampolino di attacco o una strategia per colpire una altra nazione.
- Triade con ricevente comune: indica che una nazione delle tre è un obbiettivo di alto valore per le altre due.
- Triade con aggressore: indica che una nazione delle tre è un aggressore per le altre due.

Tabella 4.1: Risultati

Tipo Triade	**N. Triadi**
Transitive	16
Fan-out	399
Fan-in	23

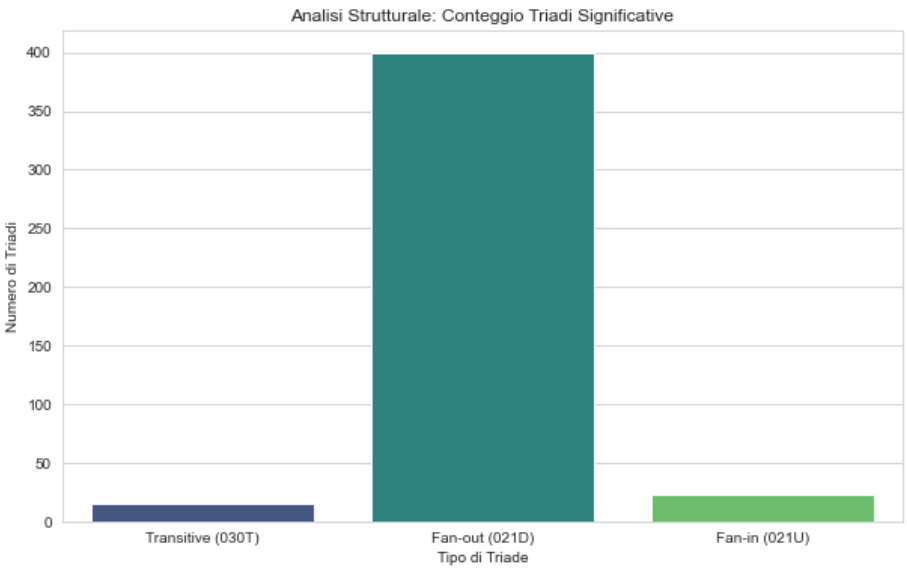

Figura 4.1: Distribuzione dei tipi di triadi

4.1.1 Esempio Triadi transitive

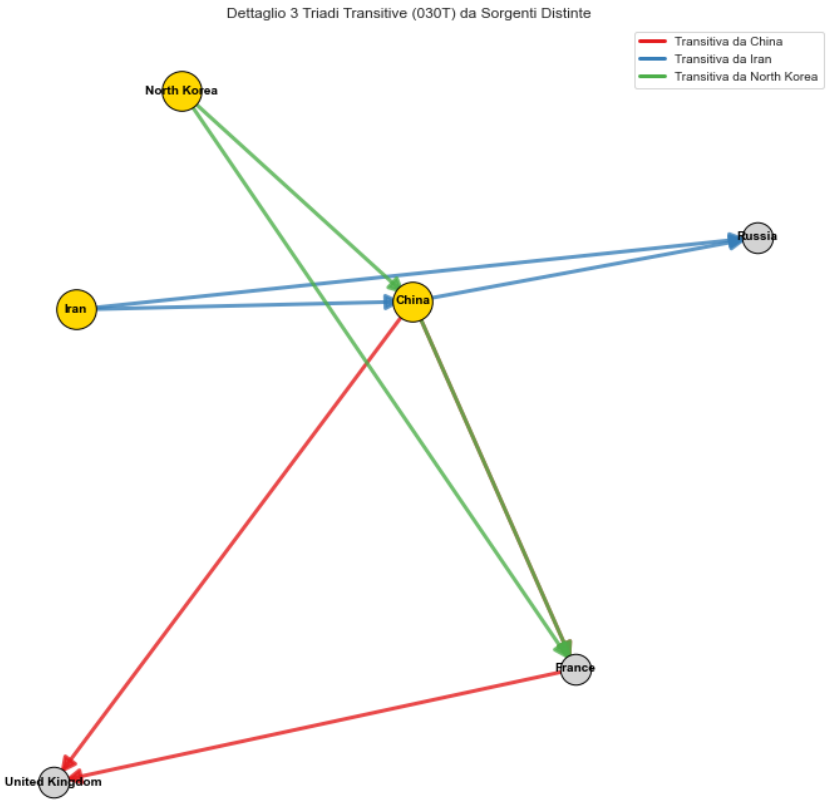

Figura 4.2: Esempio di triadi transitive

4.1.2 Esempio Triade Fan-In

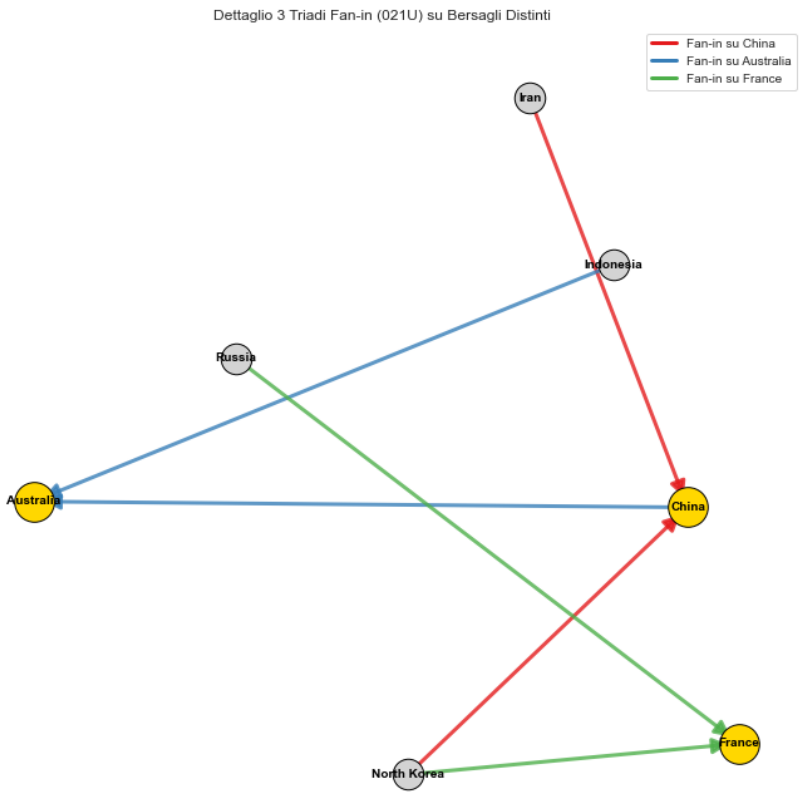

Figura 4.3: Esempio di triadi fan-in

4.1.3 Esempio Triade Fan-Out

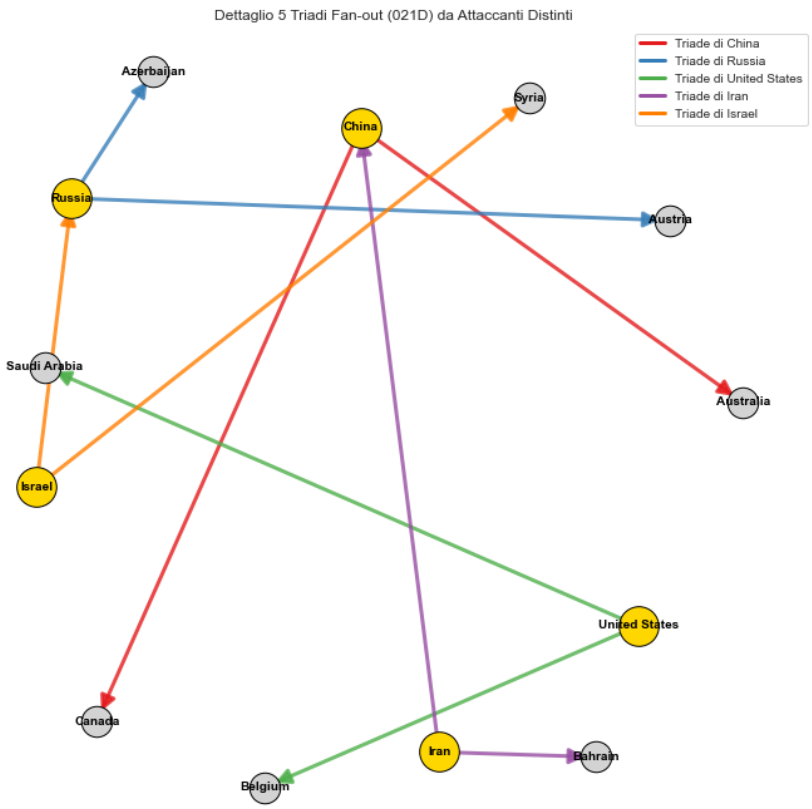

Figura 4.4: Esempio di triadi con aggressore comune

4.2 Clustering

Il clustering in un grafo orientato misura la probabilità che, se esistono relazioni tra A-B e B-C, esista anche una relazione A-C. Un valore alto di clustering indica che esiste un conflitto esteso tra più nazioni mentre un clustering basso indica una nazione che esegue o subisce attacchi isolati.

Paese	Clustering-Coeff	Degree
Paese	Clustering-Coeff	Degree
Vietnam	1.000000	3
Saudi Arabia	0.833333	3
Germany	0.500000	2
Canada	0.500000	2
Bangladesh	0.500000	2
France	0.500000	4
Italy	0.500000	2
South Korea	0.277778	5
United Kingdom	0.250000	10
Iran	0.207547	11

4.2.1 Grafico a barre distribuzione del coefficiente di clustering

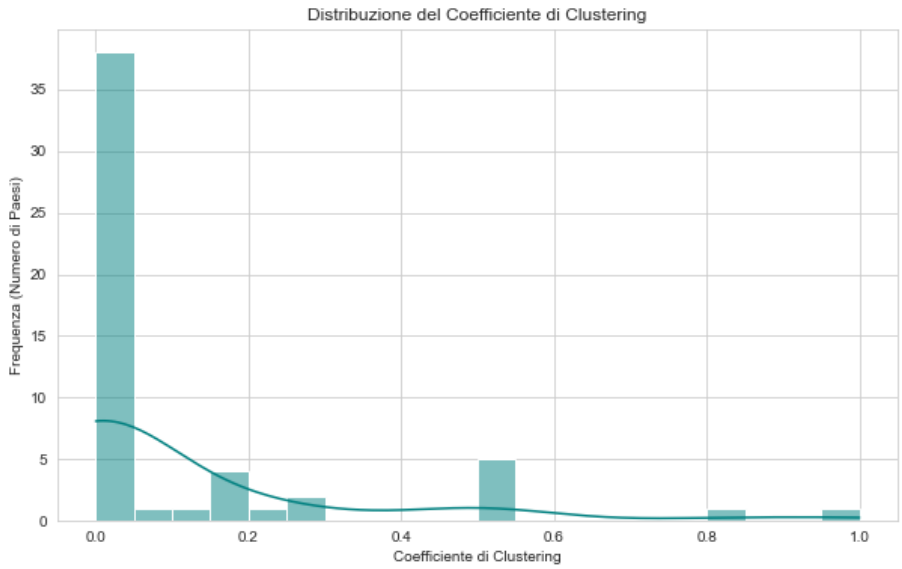

Figura 4.5: Esempio di triadi con aggressore comune

4.2.2 Degree vs Clustering

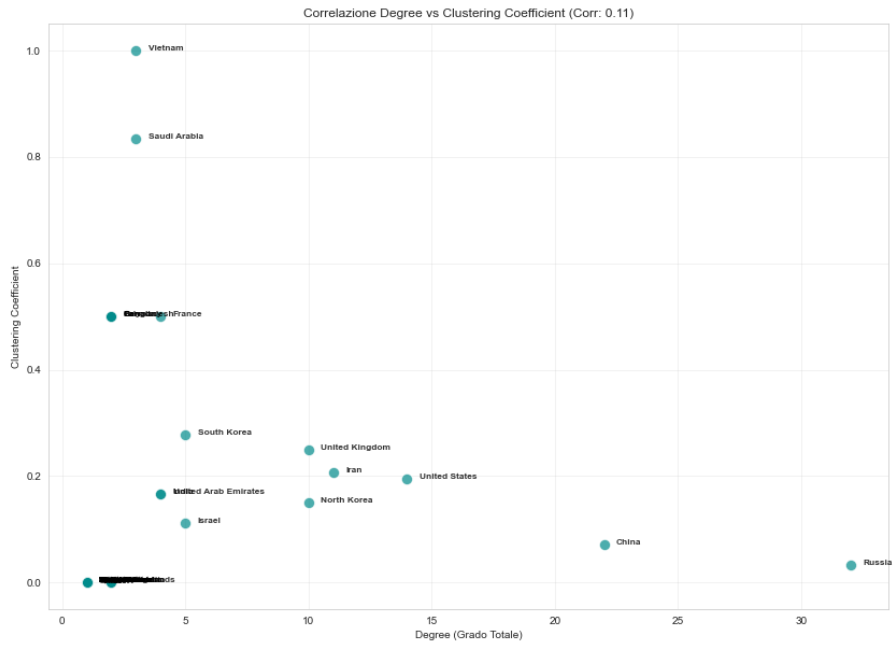

Figura 4.6: Esempio di triadi con aggressore comune

4.2.3 Conclusioni

- Il Vietnam rappresenta una anomalia o un conflitto locale altamente isolato che non ha un impatto strutturale sul resto della rete.
- United Kingdom e United States sono il fulcro del conflitto, definendo la zona con l'attività più intensa e con ruoli di ponte critici.
- Russia e Cina sono le forze che alimentano il traffico verso questo centro e la periferia, ma le loro campagne sono più sparse e meno coese a livello locale

4.3 Analisi delle Clique

Un *clique* è un sottografo massimale in cui ogni coppia di nodi è connessa. Nel contesto cyber, un clique rappresenta un insieme di paesi con conflitti cyber reciproci e documentati.

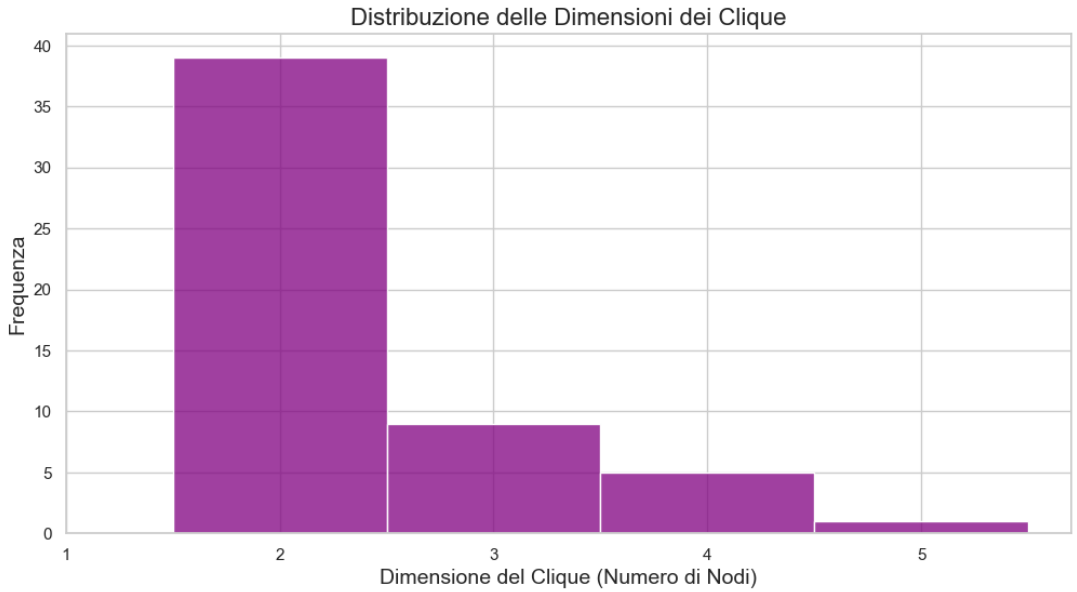

Figura 4.7: Distribuzione delle dimensioni dei clique nella rete

L'analisi dei clique rivela:

- Prevalenza di clique di dimensione 2 (39 coppie di paesi in conflitto bilaterale)
- 9 clique di dimensione 3 (conflitti trilaterali)
- 5 clique di dimensione 4 e 1 clique massimo di dimensione 5

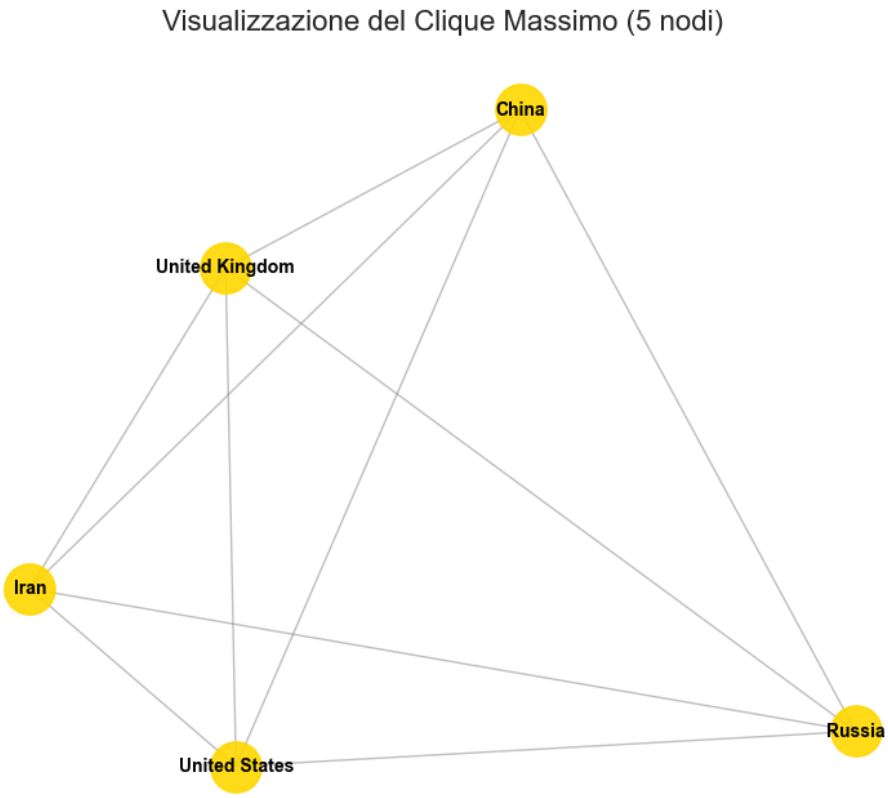

Figura 4.8: Visualizzazione del clique massimo (5 nodi): China, Russia, United Kingdom, United States, Iran - i cinque paesi più interconnessi nei conflitti cyber globali

4.4 K-Core e Decomposizione a Cipolla

Un *K-core* è un sottografo massimale in cui ogni nodo ha grado $\geq k$. La *decomposizione a cipolla* (onion decomposition) stratifica la rete in livelli concentrici di coesione crescente. Si può distinguere:

- In-K-core: in cui un alto valore di k indica nazioni che subiscono un numero massiccio di attacchi da altre nazioni che sono anch'esse pesantemente attaccate ovvero essere sistematicamente vulnerabili in un ambiente ostile.
- Out-K-Core: in cui un valore alto di k indica un gruppo di nazioni iper-aggressive che attaccano altre nazioni aggressive.
- Struttura a cipolla: in cui le nazioni periferiche (basso K) sono quelle che lanciano o subiscono attacchi sporadici.

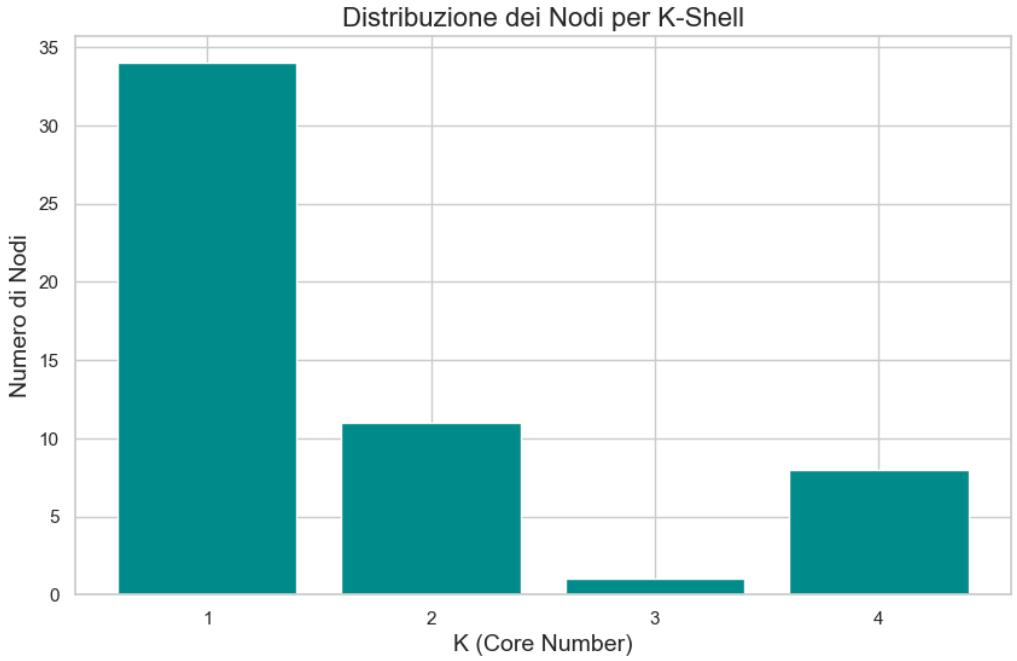

Figura 4.9: Distribuzione dei nodi per K-Shell: la maggior parte dei paesi (34) appartiene al 1-shell (periferia), mentre 8 paesi formano il 4-core centrale

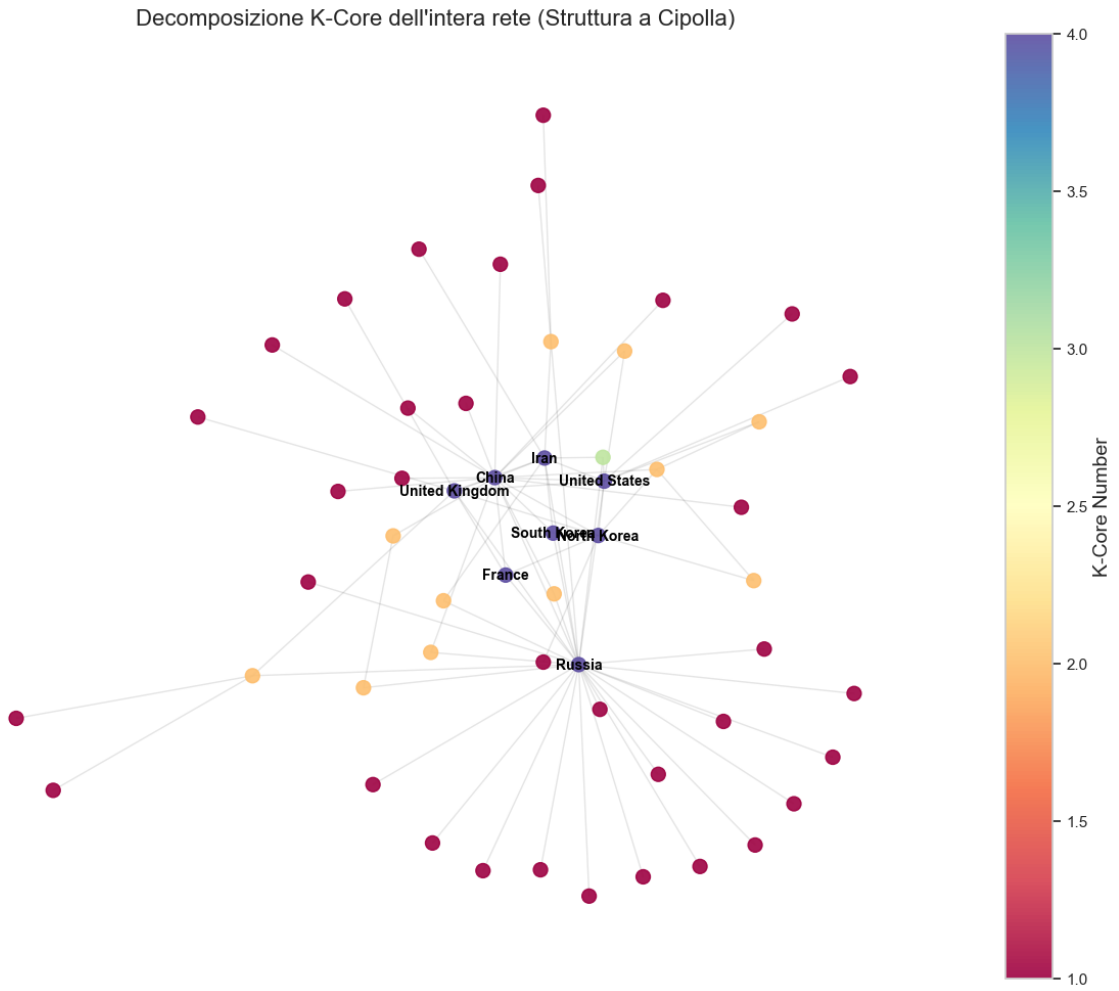

Figura 4.10: Decomposizione K-Core dell'intera rete (Struttura a Cipolla) - Il colore indica il K-Core number: i nodi centrali (k=4) sono il nucleo della rete cyber globale

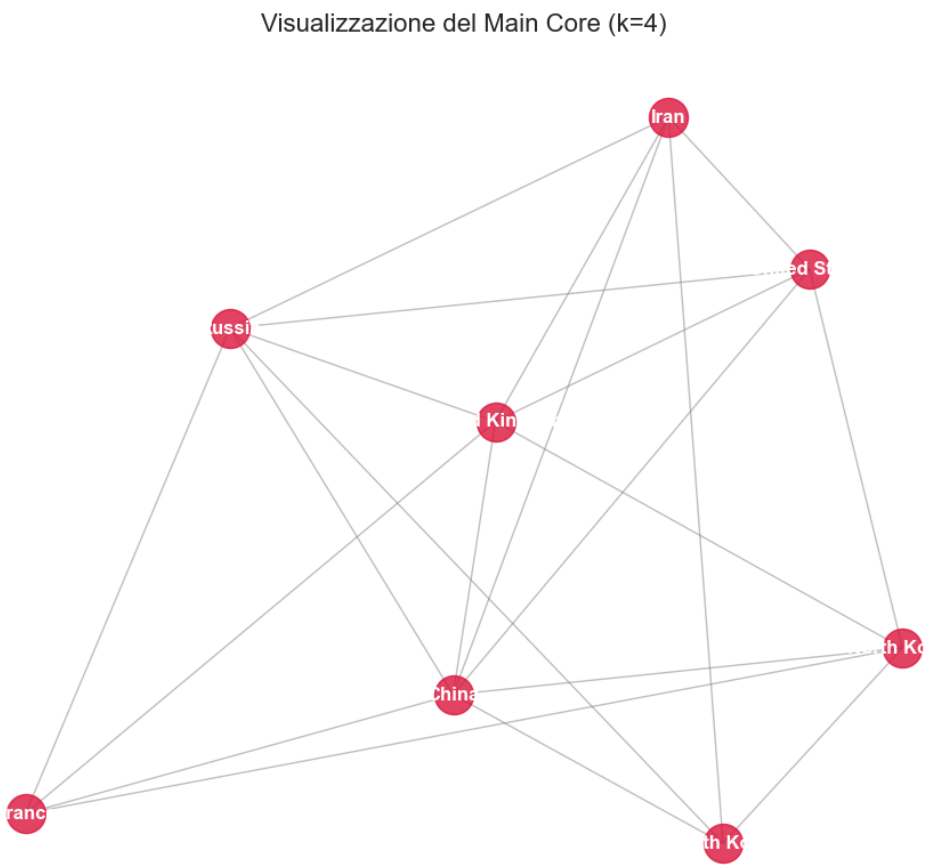

Figura 4.11: Visualizzazione del Main Core (k=4): Iran, Russia, United Kingdom, China, United States, France, North Korea, South Korea - gli 8 paesi più densamente interconnessi

4.5 Ego Networks

Una *ego network* è una rete focalizzata su un singolo nodo (”ego”) e le sue connessioni dirette (”alter”). Questa analisi permette di comprendere il ”vicinato” di ogni attore principale.

4.5.1 Ego Networks dei Top 3 Paesi Target (Vittime)

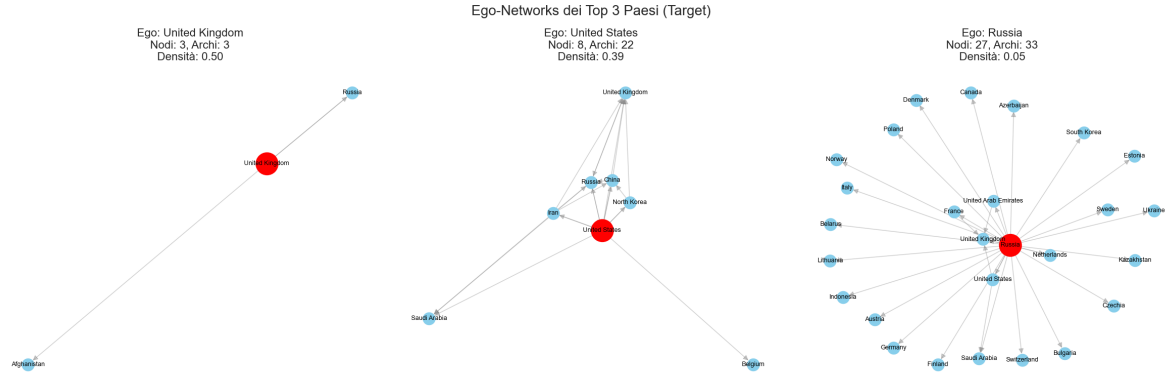

Figura 4.12: Ego-Networks dei Top 3 Paesi Target: United Kingdom (3 nodi, densità 0.50), United States (8 nodi, densità 0.39), Russia (27 nodi, densità 0.05)

4.5.2 Ego Networks dei Top 3 Paesi Attaccanti

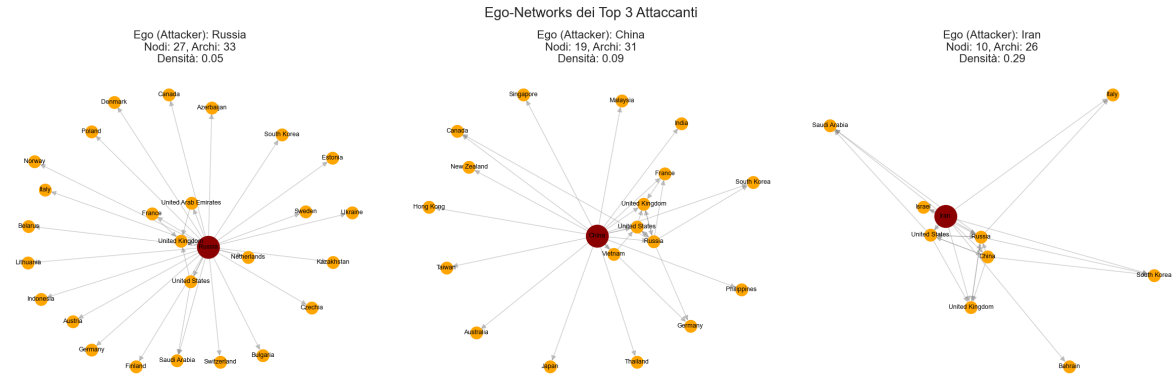

Figura 4.13: Ego-Networks dei Top 3 Attaccanti: Russia (27 nodi, densità 0.05), China (19 nodi, densità 0.09), Iran (10 nodi, densità 0.29)

L'analisi delle ego networks rivela:

- **Russia**: La più estesa (27 nodi), ma bassa densità - attacchi diffusi a molti paesi non interconnessi
- **China**: 19 nodi con focus su Asia-Pacifico e Occidente
- **Iran**: Rete più piccola (10 nodi) ma più densa - conflitti concentrati

4.6 Rilevamento delle Community

4.6.1 Focus Community Pozzo e Sorgente

- Comunità di tipo Pozzo:Gruppi di nazioni dove gli archi entrano dall'esterno ma difficilmente escono.

- Comunità di tipo Sorgente:Gruppi di nazioni da cui partono molti archi verso l'esterno, ma ne ricevono pochi dall'esterno.

Community	Size	In-Flow	Out-Flow	Role
3	20	12	37	Sorgente (Attaccante)
0	14	28	74	Sorgente (Attaccante)
2	11	89	21	Pozzo (Bersaglio)
1	6	16	13	Pozzo (Bersaglio)

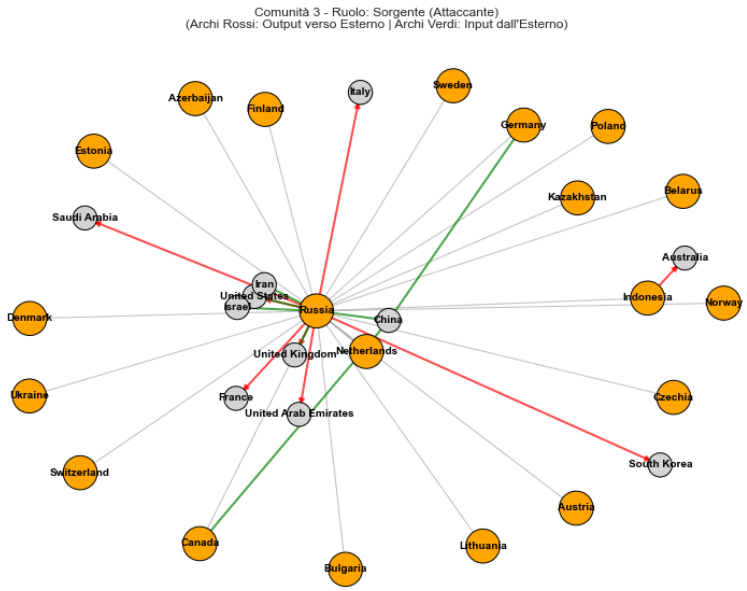

Figura 4.14: Community 3

Dettagli Comunità 3 (Sorgente (Attaccante)):
→ Stati Interni (20): Austria, Azerbaijan, Belarus, Bulgaria, Canada, Czechia, Denmark, Estonia, Finland, Germany, Indonesia, Kazakhstan, Lithuania, Netherlands, Norway, Poland, Russia, Sweden, Switzerland, Ukraine
→ Stati Esterni Interagenti (11): Australia, China, France, Iran, Israel, Italy, Saudi Arabia, South Korea, United Arab Emirates, United Kingdom, United States

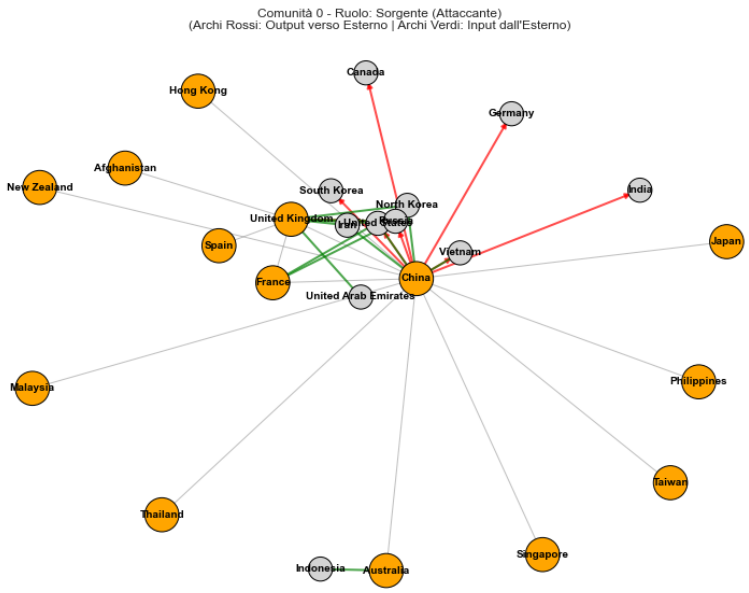

Figura 4.15: Community 0

Dettagli Comunità 0 (Sorgente (Attaccante)):
→ Stati Interni (14): Afghanistan, Australia, China, France, Hong Kong, Japan, Malaysia, New Zealand, Philippines, Singapore, Spain, Taiwan, Thailand, United Kingdom
→ Stati Esterni Interagenti (11): Canada, Germany, India, Indonesia, Iran, North Korea, Russia, South Korea, United Arab Emirates, United States, Vietnam

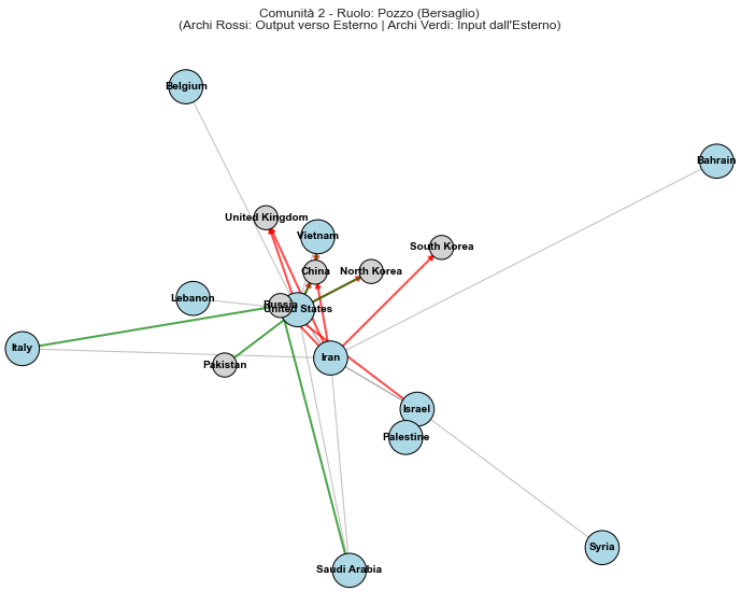

Figura 4.16: Community 2

Dettagli Comunità 2 (Pozzo (Bersaglio)):
→ Stati Interni (11): Bahrain, Belgium, Iran, Israel, Italy, Lebanon, Palestine, Saudi Arabia, Syria, United States, Vietnam
→ Stati Esterni Interagenti (6): China, North Korea, Pakistan, Russia, South Korea, United Kingdom

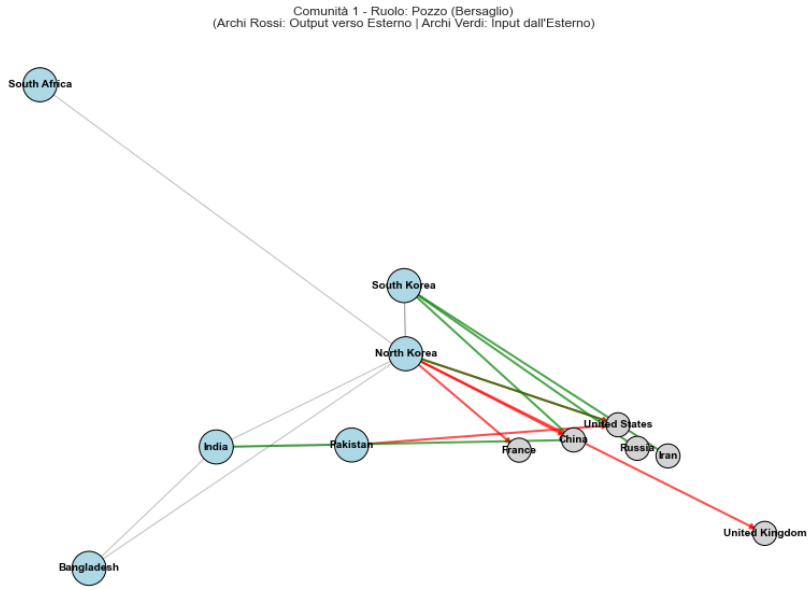

Figura 4.17: Community 1

Dettagli Comunità 1 (Pozzo (Bersaglio)):
→ Stati Interni (6): Bangladesh, India, North Korea, Pakistan, South Africa, South Korea
→ Stati Esterni Interagenti (6): China, France, Iran, Russia, United Kingdom, United States

4.6.2 Algoritmo di Louvain

L'algoritmo di Louvain massimizza la *modularità* della partizione, identificando gruppi di paesi più connessi tra loro che con il resto della rete.

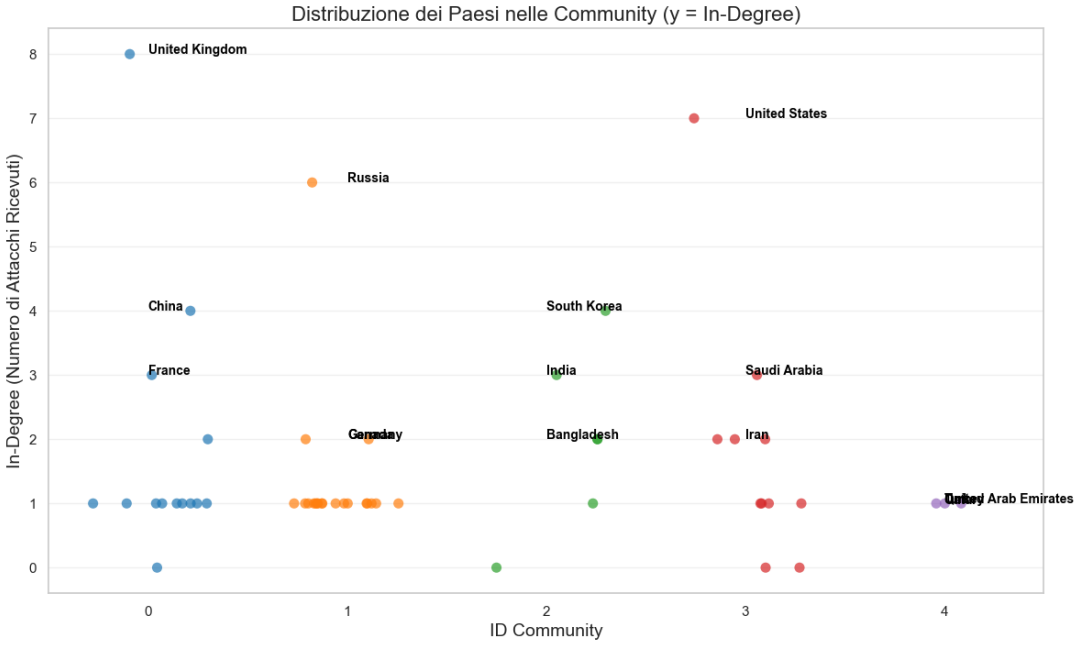

Figura 4.18: Numero di Paesi per Community (Louvain): 5 community identificate con dimensioni variabili da 3 a 20 paesi

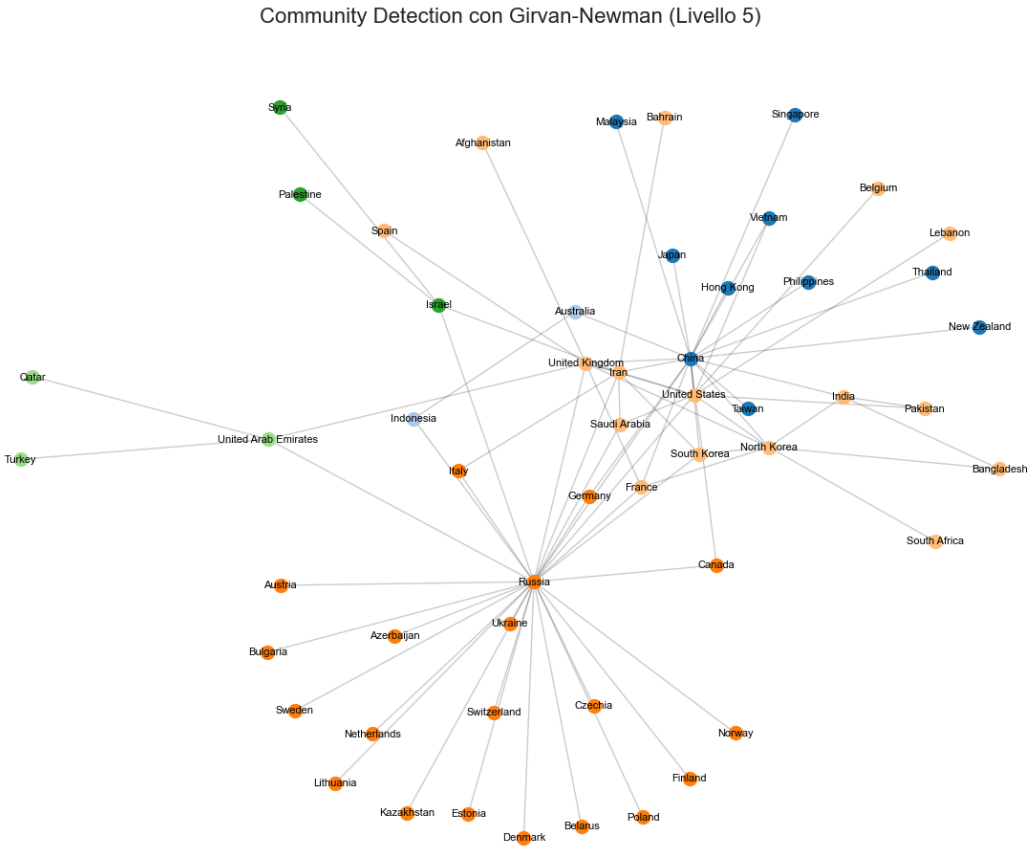

Figura 4.19: Distribuzione dei Paesi nelle Community (y = In-Degree): ogni punto è un paese, colorato per community di appartenenza

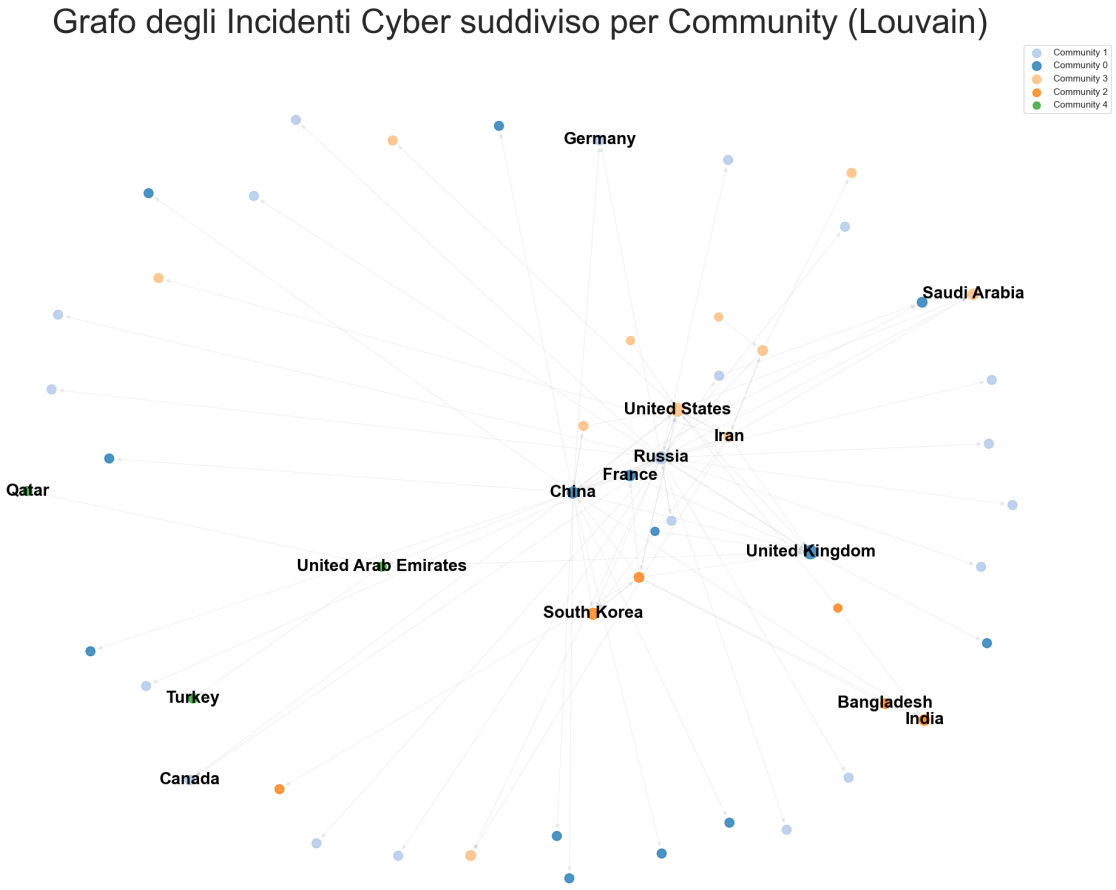

Figura 4.20: Grafo degli Incidenti Cyber suddiviso per Community (Louvain) - Spring Layout

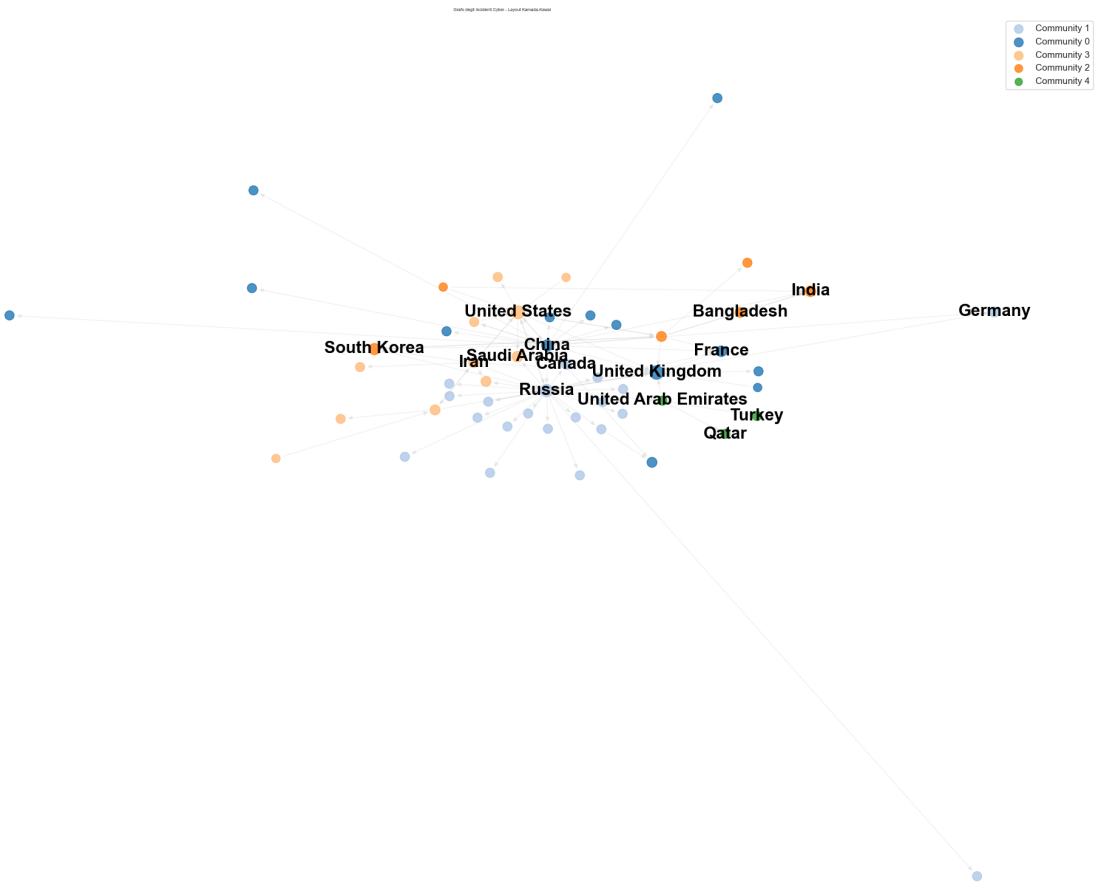

Figura 4.21: Grafo degli Incidenti Cyber - Layout Kamada-Kawai con colorazione per Community

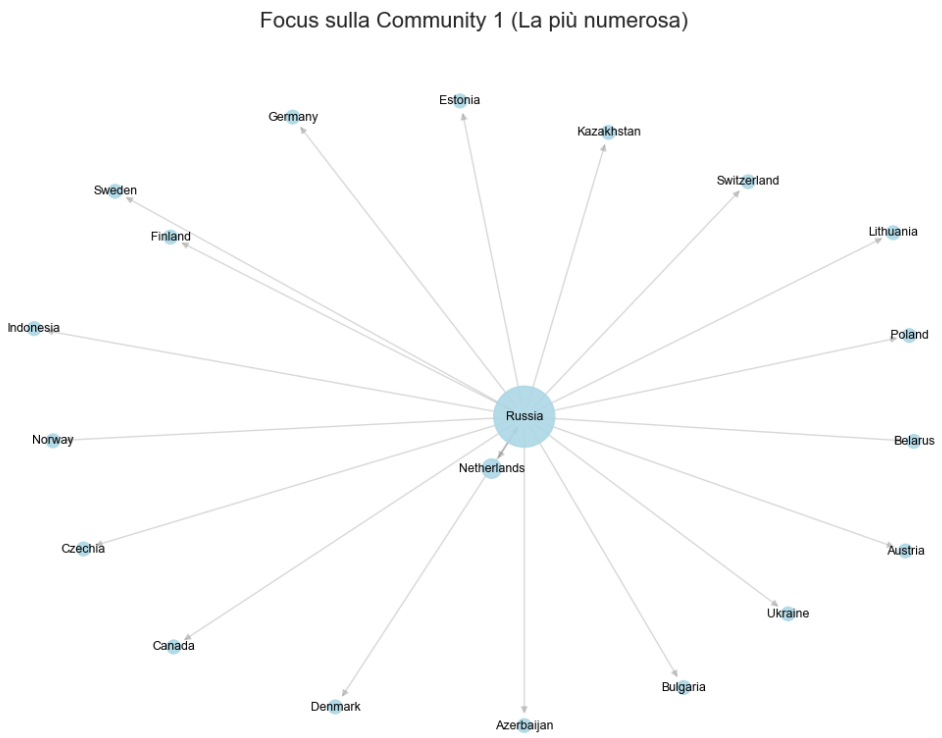

Figura 4.22: Focus sulla Community 1 (La più numerosa): Russia al centro con 20 paesi europei e dell'ex-blocco sovietico

4.6.3 Algoritmo di Girvan-Newman

L'algoritmo di *Girvan-Newman* identifica le community rimuovendo iterativamente gli archi con maggiore betweenness, "spezzando" progressivamente la rete in componenti.

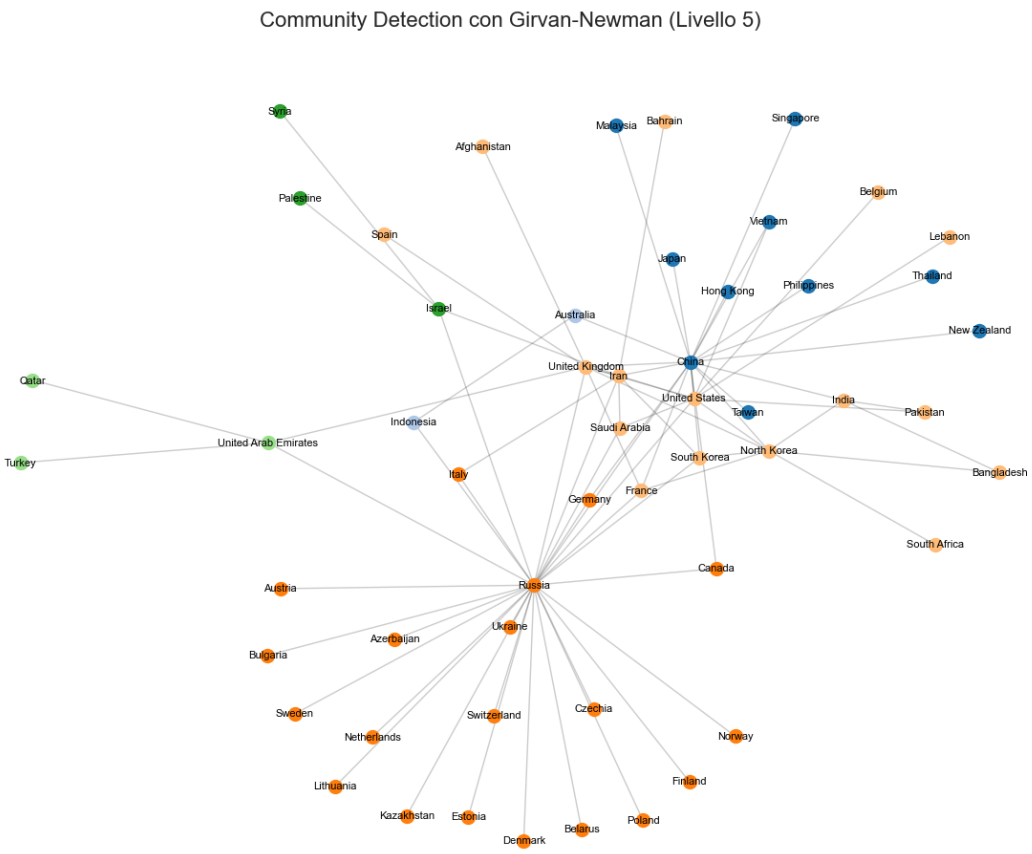

Figura 4.23: Community Detection con Girvan-Newman (Livello 5): 6 community identificate con struttura diversa da Louvain

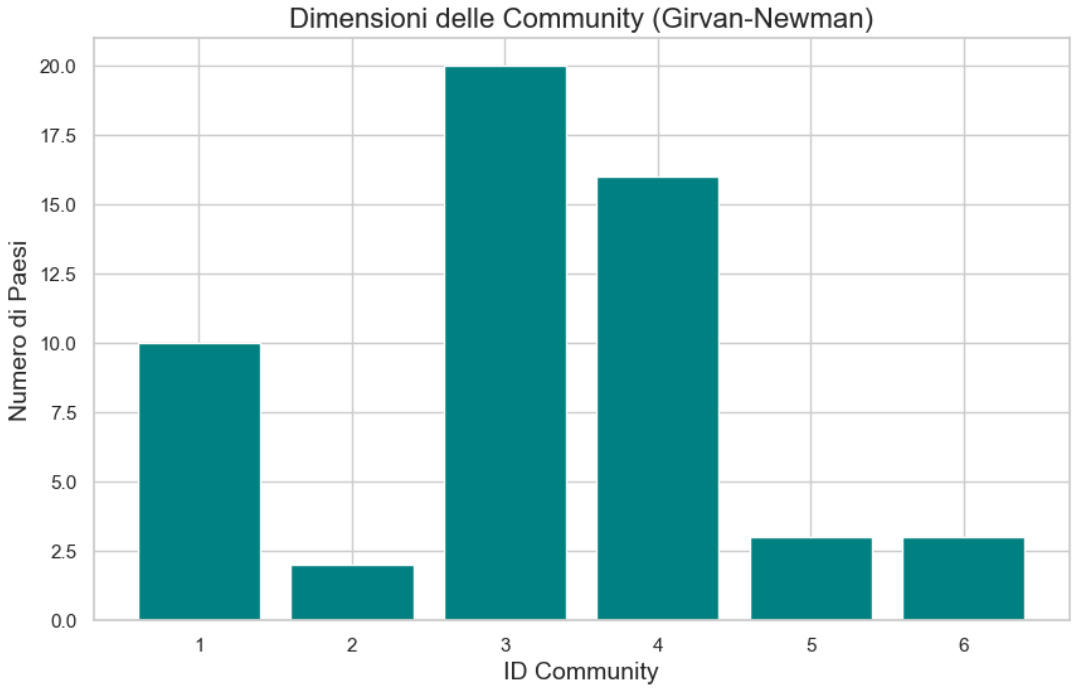

Figura 4.24: Dimensioni delle Community (Girvan-Newman): distribuzione più eterogenea rispetto a Louvain

4.7 Confronto tra Algoritmi di Community Detection

Tabella 4.2: Confronto tra Louvain e Girvan-Newman

Caratteristica	Louvain	Girvan-Newman
Numero di Community	5	6
Community più grande	20 paesi	20 paesi
Community più piccola	3 paesi	2 paesi
Approccio	Ottimizzazione modularità	Rimozione edge betweenness
Complessità	O(n log n)	O(m² n)

4.8 Interpretazione Geopolitica delle Strutture

Le strutture identificate hanno significato diretto nell'analisi geopolitica:

- **Clique Massimo (5 paesi)**: China, Russia, UK, USA, Iran - rappresenta il "pentagono" dei conflitti cyber globali
- **4-Core (8 paesi)**: Include anche France, North Korea, South Korea - il nucleo delle operazioni cyber statali
- **Community Russia-centrica**: Riflette la sfera di influenza russa e i target preferenziali

- **Community US-centrica**: Include alleati NATO e target asiatici
- **Ego Network Iran**: Conflitti concentrati con USA, Israel, Saudi Arabia - riflette tensioni mediorientali